

# Linear Network Coding over Rings

## Part II: Vector Codes and Non-Commutative Alphabets \*

Joseph Connelly and Kenneth Zeger

*IEEE Transactions on Information Theory*

*Submitted: August 5, 2016*

### Abstract

We prove the following results regarding the linear solvability of networks over various alphabets. For any network, the following are equivalent: (i) vector linear solvability over some finite field, (ii) scalar linear solvability over some ring, (iii) linear solvability over some module. Analogously, the following are equivalent: (a) scalar linear solvability over some finite field, (b) scalar linear solvability over some commutative ring, (c) linear solvability over some module whose ring is commutative. Whenever any network is linearly solvable over a module, a smallest such module arises in a vector linear solution for that network over a field.

If a network is linearly solvable over some non-commutative ring but not over any commutative ring, then such a non-commutative ring must have size at least 16, and for some networks, this bound is achieved. An infinite family of networks is demonstrated, each of which is scalar linearly solvable over some non-commutative ring but not over any commutative ring.

Whenever  $p$  is prime and  $2 \leq k \leq 6$ , if a network is scalar linearly solvable over some ring of size  $p^k$ , then it is also  $k$ -dimensional vector linearly solvable over the field  $\text{GF}(p)$ , but the converse does not necessarily hold. This result is extended to all  $k \geq 2$  when the ring is commutative.

---

\*This work was supported by the National Science Foundation.

**J. Connelly and K. Zeger** are with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA 92093-0407 (j2connelly@ucsd.edu and zeger@ucsd.edu).

# 1 Introduction

In the companion paper (i.e. Part I) [2], we studied scalar linear network codes over commutative rings. Equivalently, these are linear codes over modules where a commutative ring acts on its own additive group via multiplication in the ring. In particular, we compared the scalar linear solvability of networks over different types of commutative rings of the same size. We proved that networks that are scalar linearly solvable over some commutative ring are also scalar linearly solvable over some field, although not necessarily of the same size. Additionally, we characterized all commutative rings with the property that there exists a network with a scalar linear solution over the ring but not over any other commutative ring of the same size.

Linear network codes can be advantageous due to their ease of implementation and mathematical tractability. These properties are due to the algebraic simplicity of linear maps and also to the structured nature of the alphabets used. Fields have the most algebraic constraints among alphabets used for linear network coding, e.g. associativity, distributivity, commutativity, invertibility. More generally, rings may lack commutativity and/or invertibility, thus providing a broader class of alphabets over which to achieve linear network solvability. We demonstrated in Part I that relaxing only the invertibility constraint (i.e. restricting to commutative rings) can lead to linear network solvability that would not otherwise be possible with fields of the same alphabet size.

In the present paper (Part II), we additionally relax the commutativity constraint, and we study linear coding over general ring alphabets and, even more generally, over modules. Vector and scalar linear codes over rings and fields are special cases of linear codes over modules. We focus on the relationship between alphabet commutativity and the scalar and vector linear solvability of networks, and we compare the linear solvability of networks over different modules where the alphabet size is the same.

## 1.1 Linear codes over modules

**Definition 1.1.** An  $R$ -module (specifically a left  $R$ -module) is an Abelian group  $(G, \oplus)$  together with a ring<sup>1</sup>  $(R, +, *)$  of *scalars* and an action

$$\cdot : R \times G \rightarrow G$$

such that for all  $r, s \in R$  and all  $g, h \in G$  the following hold:

$$\begin{aligned} r \cdot (g \oplus h) &= (r \cdot g) \oplus (r \cdot h) \\ (r + s) \cdot g &= (r \cdot g) \oplus (s \cdot g) \\ (r * s) \cdot g &= r \cdot (s \cdot g) \\ 1 \cdot g &= g. \end{aligned}$$

For brevity, we will sometimes refer to such an  $R$ -module as  ${}_R G$  or simply  $G$ . The *size of a module* will refer to  $|G|$ . Let  $M_k(R)$  denote the ring of all  $k \times k$  matrices with entries in  $R$  and let

---

<sup>1</sup>In this paper we will assume all groups are finite and all rings have a multiplicative identity, even when we do not explicitly state these facts.

$G^k$  denote the Abelian group of all  $k$ -dimensional vectors with entries in  $G$  with vector addition, where  $k$  is a positive integer. Then  $G^k$  is an  $M_k(R)$ -module where multiplication of elements of  $R$  with elements of  $G$  is given by the action of  ${}_RG$ .

For basic network coding definitions, see Part I [2, Section 1.1]. We will use the same models as in Part I for networks, alphabets, etc., except we now study the generalized case of linear codes over modules, as opposed to linear codes over rings. An edge function on the out-edge of a network node is *linear with respect to the module*  ${}_RG$  if it can be written in the form

$$f(x_1, \dots, x_m) = (M_1 \cdot x_1) \oplus \dots \oplus (M_m \cdot x_m) \quad (1)$$

where  $x_1, \dots, x_m \in G$  are the inputs of the node and  $M_1, \dots, M_m \in R$  are constants. That is, the messages and edge symbols are elements of the Abelian group  $G$ , and the linear edge and decoding functions are determined by coefficients of the ring  $R$ . A decoding function is linear with respect to  ${}_RG$  if it has a form analogous to (1), and a code is *linear over a module*  ${}_RG$  if all edge and decoding functions are linear with respect to  ${}_RG$ . The alphabet size in a linear code over a module is the size of the module, i.e.  $|G|$ . The special case of a module where the finite ring  $R$  acts on its own Abelian group  $(R, +)$  by multiplication in  $R$  is denoted by  ${}_RR$ , and in this case, (1) is equivalent to the definition of a scalar linear code over a ring that we used in Part I.

A network is *linearly solvable over a module*  ${}_RG$  if there exists a linear solution over  ${}_RG$ . We will focus on two special types of linear codes:

- (i) A *scalar linear code over a ring*  $R$  is a linear code over the module  ${}_RR$ . A network is *scalar linearly solvable over*  $R$  if it has a linear solution over the module  ${}_RR$ .
- (ii) A  *$k$ -dimensional vector linear code over a ring*  $R$  is a linear code over the module  ${}_{M_k(R)}R^k$ . A network is *vector linearly solvable over*  $R$  if it has a linear solution over the module  ${}_{M_k(R)}R^k$ , for some positive integer  $k$ .

When referring to a linear code or solution over a ring, we will always specify (in this paper) scalar versus vector, or if neither is specified, then we are referring to a linear code over a module. Additionally, when referring to an  $R$ -module  $G$ , the ring  $R$  is not assumed to be finite, unless otherwise specified. However, when referring to a scalar or vector linear code over a ring  $R$ , the ring  $R$  is assumed to be finite.

A  *$k$ -dimensional vector routing code over an alphabet*  $\mathcal{A}$  is a code in which messages and edge symbols are elements of  $\mathcal{A}^k$  and edge and decoding functions copy certain input vector components to the certain output vector components. A vector routing code over  $\mathcal{A}$  is, in fact, a special case of a vector linear code over  $\mathcal{A}$  where each row of each of the matrices  $M_1, \dots, M_m$  in (1) is either all zero or else has 1 one and  $k - 1$  zeros, and for each  $i \leq k$ , at most one of the matrices  $M_1, \dots, M_m$  has a non-zero  $i$ th row.

We can similarly define a right  $R$ -module and a linear code over a right  $R$ -module. It can easily be shown that any linear code over a right module is equivalent to a particular linear code over a left module, so we restrict attention only to left modules.

## 1.2 Our contributions

In Section 1.3, lemmas are given which are used in proofs later in the paper.

Section 2 analyzes the linear solvability of networks over ring alphabets which are not necessarily commutative. In Part I, we proved that whenever a network is scalar linearly solvable over some commutative ring, then the smallest commutative ring over which the network is scalar linearly solvable is a field (and thus the ring is unique) [2, Theorem 2.5]. Here, we prove (in Theorem 2.5) that if a network is scalar linearly solvable over some (not necessarily commutative) ring, then a smallest such ring is a matrix ring over a field. It remains unknown, however, whether there can be more than one smallest (not necessarily commutative) ring over which a network is linearly solvable, since in general, there can exist multiple matrix rings over fields that are the same size. We demonstrate (in Corollaries 2.14 and 3.8) that for two infinite classes of networks studied in this paper, the smallest size ring over which each network is linearly solvable is indeed unique.

We prove (in Theorem 2.10) that if a network is linearly solvable over some module, then a smallest such module (i.e. with a smallest associated Abelian group) corresponds to a vector linear solution over some finite field.<sup>2</sup> We prove (in Theorem 2.13), in contrast to the commutative ring case, that the minimum size module with respect to linear solvability is not necessarily unique. Thus, for a fixed network, vector linear codes over fields are “best” in a certain sense, as these codes can minimize the alphabet size needed for a linear solution.

We also show (in Corollary 2.15) that for all networks, the following properties are equivalent: (i) vector linear solvability over some field, (ii) scalar linear solvability over some ring, and (iii) linear solvability over some module. Similarly, we show (in Corollary 2.16) that for all networks, the following properties are equivalent: (a) scalar linear solvability over some field, (b) scalar linear solvability over some commutative ring, and (c) linear solvability over some module whose ring is commutative.

In Section 3, we present a family of networks that generalize the M Network of [6, 14], and we enumerate (in Theorem 3.6) the particular vector dimensions over which each of these networks has vector linear solutions. We prove (in Corollary 3.7) that these networks have scalar linear solutions over certain non-commutative matrix rings yet do not have scalar linear solutions over any commutative ring. We also show (in Theorem 3.10) that if a network is scalar linearly solvable over a non-commutative ring  $R$  and is not scalar linearly solvable over any commutative ring, then  $|R| \geq 16$ . This lower bound is shown to be achievable (in Corollary 3.7 and Example 3.9) by exhibiting a network which has a scalar linear solution over a non-commutative ring of size 16 but not over any commutative ring.

Section 4 focuses on linear solvability of networks over different modules with the same alphabet size, specifically,  $k$ -dimensional vector linear codes over  $\text{GF}(p)$  and rings of size  $p^k$ . We prove (in Theorem 4.1) that for each prime power  $p^k$ , there exists a network with a linear solution over a module of size  $p^k$  but with no scalar linear solutions over any ring of size  $p^k$ . These particular networks have  $k$ -dimensional vector linear solutions over  $\text{GF}(p)$ . We show (in Theorem 4.4) that any network with a scalar linear solution over a commutative ring of size  $p^k$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . We prove a similar result (in Theorem 4.15) for general rings of size  $p^k$  when  $k \leq 6$ . Additionally, we show (in Theorems 4.4 and 4.15) that these results generalize in a natural way to rings of non-power-of-prime sizes.

Finally, Section 5 provides some concluding remarks.

---

<sup>2</sup>For example, in a  $k$ -dimensional vector linear code over a field  $\mathbb{F}$ , the alphabet size of the module is  $|\mathbb{F}|^k$ .

### 1.3 Comparisons of modules

An  $R$ -module  $G$  is *faithful* if for all  $r \in R \setminus \{0\}$ , there exists  $g \in G$  such that  $r \cdot g \neq 0$ . In other words,  $r \cdot g = 0$  for all  $g$  if and only if  $r = 0$ . For any finite ring  $R$  and positive integer  $k$ , the  $M_k(R)$ -module  $R^k$  is faithful, so vector and scalar linear codes over rings are special cases of linear codes over faithful modules.

For a fixed ring  $R$ , there are generally multiple modules over  $R$ . For example, if  $R$  is a subring of  $S$ , then  $(S, +)$  is an  $R$ -module where the action is multiplication in  $S$ , and  $(R, +)$  is also an  $R$ -module where the action is multiplication in  $R$ . The following lemma shows that the linear solvability of a network over a faithful  $R$ -module is determined entirely by the ring of scalars  $R$  and not by the module's underlying Abelian group. However, we note that not every ring and group pair can form a module. For example, the additive group of  $\text{GF}(2)$  cannot be a  $\text{GF}(3)$ -module, since  $1 + 1 = 0$  in  $\text{GF}(2)$  and  $1 + 1 \neq 0$  in  $\text{GF}(3)$ .

**Lemma 1.2.** *Let  $R$  be a fixed ring. If a network is linearly solvable over some faithful  $R$ -module, then it is linearly solvable over every  $R$ -module.*

*Proof.* Let  $\mathcal{N}$  be a network that is linearly solvable over the faithful  $R$ -module  $(G, \oplus)$ , and let  $z_1, \dots, z_m \in G$  denote the messages of  $\mathcal{N}$ . Suppose a node in  $\mathcal{N}$  has inputs  $x_1, \dots, x_n \in G$  in a solution over  ${}_R G$ , where, for each  $i = 1, \dots, n$ ,

$$x_i = (A_{i,1} \cdot z_1) \oplus \dots \oplus (A_{i,m} \cdot z_m)$$

for some  $A_{i,1}, \dots, A_{i,m} \in R$ . Then for each out-edge of this node, there exist constants  $B_1, \dots, B_n \in R$  such that the edge carries the symbol

$$\bigoplus_{i=1}^n (B_i \cdot x_i) = \bigoplus_{i=1}^n \bigoplus_{j=1}^m ((B_i A_{i,j}) \cdot z_j) = \bigoplus_{j=1}^m \left( \left( \sum_{i=1}^n B_i A_{i,j} \right) \cdot z_j \right).$$

Then, by induction, every edge and decoding function in a linear code over a module is a linear combination of the network messages.

$G$  is a faithful  $R$ -module, so 1 and 0 are the only elements of  $R$  such that  $1 \cdot g = g$  and  $0 \cdot g = 0$  for all  $g \in G$ . Hence it must be the case that decoding functions in the linear solution over  ${}_R G$  are of the form

$$(1 \cdot z_i) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^n (0 \cdot z_j).$$

If  $H$  is some other  $R$ -module, then a linear solution for  $\mathcal{N}$  over  ${}_R G$  is also a linear solution for  $\mathcal{N}$  over  ${}_R H$ , since every edge will carry the same linear combination of the messages (i.e. the same elements of  $R$  are the coefficients in the linear combination), so, in particular, the decoding functions will be the same linear combination of the messages. ■

In contrast to Lemma 1.2, if  $G$  is both an  $R$ -module and an  $S$ -module, then there may exist a network that is linearly solvable over  ${}_S G$  but not  ${}_R G$ . For example,  $\text{GF}(2)$  is a subfield of

$\text{GF}(4)$ , so  $(\text{GF}(4), +)$  is both a faithful  $\text{GF}(2)$ -module and a faithful  $\text{GF}(4)$ -module. We demonstrate (in Corollary 2.14) a network that is scalar linearly solvable over  $\text{GF}(4)$  but not  $\text{GF}(2)$ , and by Lemma 1.2, this network is linearly solvable over the  $\text{GF}(4)$ -module  $(\text{GF}(4), +)$  but not the  $\text{GF}(2)$ -module  $(\text{GF}(4), +)$ .

The following corollary is a special case of Lemma 1.2 and will be frequently used in later proofs. It demonstrates an equivalence between scalar linear solutions over matrix rings and vector linear solutions over rings.

**Corollary 1.3.** *Let  $R$  be a finite ring,  $k$  a positive integer, and  $\mathcal{N}$  a network. Then  $\mathcal{N}$  is scalar linearly solvable over the ring of  $k \times k$  matrices whose elements are from  $R$  if and only if  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $R$ .*

*Proof.* The “if” and the “only if” directions are each obtained by separately applying Lemma 1.2, since  $M_k(R)$  and  $R^k$  are faithful  $M_k(R)$ -modules with matrix-matrix multiplication and matrix-vector multiplication, respectively. ■

Note that in a  $k$ -dimensional vector linear code over a ring  $R$ , the alphabet size is  $|R|^k$ , whereas in a scalar linear solution over  $M_k(R)$ , the alphabet size is  $|R|^{k^2}$ . So any network that is scalar linearly solvable over the matrix ring  $M_k(R)$  is also linearly solvable over a smaller module alphabet. We will generalize this idea in Theorem 2.10.

As is common in mathematics literature, it will be assumed throughout this paper that ring homomorphisms preserve both additive and multiplicative identities.

**Lemma 1.4.** *If  $\phi : R \rightarrow S$  is a ring homomorphism and network  $\mathcal{N}$  is linearly solvable over some faithful  $R$ -module, then  $\mathcal{N}$  is linearly solvable over every  $S$ -module.*

*Proof.* Let  $H$  be an  $S$ -module and define a mapping  $\odot : R \times H \rightarrow H$  by  $r \odot h = \phi(r) \cdot h$ , where  $\cdot$  is the action of  ${}_S H$ . One can verify that  $H$  is an  $R$ -module under  $\odot$ . Now, let  $G$  be a faithful  $R$ -module, and suppose  $\mathcal{N}$  has a linear solution over  ${}_R G$ . By Lemma 1.2,  $\mathcal{N}$  is linearly solvable over  ${}_R H$ , so every edge function in the solution over  ${}_R H$  is of the form

$$y' = (M_1 \odot x_1) \oplus \cdots \oplus (M_m \odot x_m) \quad (2)$$

where  $x_1, \dots, x_m \in H$  are the parent node’s inputs and  $M_1, \dots, M_m \in R$  are constants.

Form a linear code for  $\mathcal{N}$  over  ${}_S H$  by replacing each coefficient  $M_i$  in (2) by  $\phi(M_i)$ . Let  $y$  be the edge symbol in the code over  ${}_S H$  corresponding to  $y'$  in the code over  ${}_R H$ . Then

$$\begin{aligned} y &= (\phi(M_1) \cdot x_1) \oplus \cdots \oplus (\phi(M_m) \cdot x_m) \\ &= (M_1 \odot x_1) \oplus \cdots \oplus (M_m \odot x_m) = y'. \end{aligned}$$

Thus, whenever an edge function in the solution over  ${}_R H$  outputs the symbol  $y'$ , the corresponding edge function in the code over  ${}_S H$  will output the same symbol  $y'$ . Likewise, whenever  $x$  is an input to an edge function in the solution over  ${}_R H$ , the corresponding input of the corresponding edge function in the code over  ${}_S H$  will be the same symbol  $x$ . The same argument holds for the decoding functions in the code over  ${}_S H$ , so each receiver will correctly obtain its corresponding demands in the code over  ${}_S H$ . Hence, the code over  ${}_S H$  is a linear solution for  $\mathcal{N}$ . ■

**Corollary 1.5.** *Let  $R$  and  $S$  be finite rings. If there exists a ring homomorphism from  $R$  to  $S$ , then every network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $S$ .*

*Proof.*  $(R, +)$  is a faithful  $R$ -module for any finite ring  $R$ , so this is a special case of Lemma 1.4 where the modules are  ${}_R R$  and  ${}_S S$ . ■

For finite rings  $R$  and  $S$ , special cases of Corollary 1.5 include:

- (1)  $S$  is a subring of  $R$ :

The identity mapping is an injective homomorphism from  $S$  to  $R$ , so any network that is scalar linearly solvable over  $S$  is also scalar linearly solvable over  $R$ .

- (2)  $R$  has a two-sided ideal  $I$ :

There is a surjective homomorphism from  $R$  to  $R/I$  (see Lemma 2.2), so any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $R/I$ .

- (3)  $\phi : R \times S \rightarrow R$  is the projection mapping:

$\phi$  is a surjective homomorphism, so any network that is scalar linearly solvable over  $R \times S$  is also scalar linearly solvable over  $R$  (and likewise over  $S$ ).

Cases (1), (2), and (3) agree with Lemma 2.8, Corollary 2.4, and Lemma 2.6, respectively, from Part I. In fact, Corollary 1.5 is a generalization of these results.

## 2 Commutative and non-commutative rings

We will focus on linear codes over modules whose ring acts on its own Abelian group, i.e. scalar linear codes over rings. As noted after Corollary 1.5, for any two-sided ideal  $I$  of a finite ring  $R$ , every network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $R/I$ , so in determining the smallest ring over which a network is scalar linearly solvable, it is natural to focus attention on rings without two-sided ideals.

A ring is *simple* if it has no proper two-sided ideals. That is, its only two-sided ideals are the ring itself and the trivial ideal  $\{0\}$ . The following lemmas give results related to simple rings and network linear solvability.

**Lemma 2.1.** *A finite ring is simple if and only if it is isomorphic to a matrix ring over a field.*

*Proof.* This is a corollary of the Artin-Wedderburn theorem (e.g. [12, p. 36, Theorem 3.10 (4)] and [13, p. 20, Theorem II.9]). ■

**Lemma 2.2.** [7, Theorem 7, p. 243] *If  $I$  is a two-sided ideal of ring  $R$ , then the mapping  $\phi : R \rightarrow R/I$  given by  $\phi(x) = x + I$  is a surjective homomorphism.*

**Lemma 2.3.** *For each finite ring  $R$ , there exists a simple ring  $S$  such that the following hold:*

- (a) *there exists a surjective homomorphism from  $R$  to  $S$ ,*
- (b) *every network that is scalar linearly solvable over  $R$  is scalar linearly solvable over  $S$ , and*
- (c)  *$|S|$  divides  $|R|$ .*

*Proof.* If  $R$  is a simple ring, then each statement is trivially true by taking  $S = R$ , so we may assume  $R$  is not a simple ring. Thus,  $R$  has a proper maximal two-sided ideal  $I$ . Let  $S = R/I$ , and note that since  $I$  is maximal,  $S$  is simple. The mapping  $\phi : R \rightarrow R/I$  given by  $\phi(x) = x + I$  is a surjective homomorphism by Lemma 2.2, which proves (a). Hence by Corollary 1.5, any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $S$ , which proves (b). Since  $R$  is finite, we know that  $|R/I|$  divides  $|R|$ , which proves (c). ■

If  $R$  is a finite commutative ring and  $S$  is a simple ring satisfying (a)-(c) in Lemma 2.3, then  $S$  must also be commutative, since there is a surjective homomorphism from  $R$  to  $S$ . However, as we demonstrate in the following example, if  $R$  is non-commutative, then such an  $S$  is not necessarily non-commutative.

**Example 2.4.** *The following demonstrates: (i) a class of non-commutative rings for which the simple ring in Lemma 2.3 is non-commutative, and (ii) a class of non-commutative rings for which the simple ring in Lemma 2.3 is commutative*

- (i) *Let  $\mathbf{Z}_n$  denote the ring of integers mod  $n$ . For any positive integers  $k, n$ , and prime divisor  $p$  of  $n$ , there exists a surjective homomorphism from the non-commutative ring  $M_k(\mathbf{Z}_n)$  to the non-commutative simple ring  $M_k(\mathbf{Z}_p)$ , given by matrix-component-wise reduction mod  $p$ .*
- (ii) *For each field  $\mathbb{F}$  and integer  $k \geq 2$ , there exists a surjective homomorphism from the non-commutative ring of upper triangular  $k \times k$  matrices with entries in  $\mathbb{F}$  to the commutative simple ring  $\mathbb{F}$  (see the proof of Lemma 4.8).*



The following theorem demonstrates that any smallest ring over which a network is scalar linearly solvable is simple.

**Theorem 2.5.** *If a network is scalar linearly solvable over a ring  $R$  but not over any smaller ring, then  $R$  is a matrix ring over a field.*

*Proof.* Suppose a network  $\mathcal{N}$  is scalar linearly solvable over a ring  $R$  that is not simple. By Lemma 2.3 (a) (b), there exists a simple ring  $S$  and a surjective homomorphism  $\phi : R \rightarrow S$ , such that  $\mathcal{N}$  is scalar linearly solvable over  $S$ . Since  $\phi$  is surjective,  $|R| \geq |S|$ , but since  $S$  is simple and  $R$  is not, the two rings cannot be isomorphic, so  $|R| \neq |S|$ , and therefore  $|R| > |S|$ .

This proves that every smallest size ring over which  $\mathcal{N}$  is scalar linearly solvable must be simple, which implies that such a ring is a matrix ring over a field by Lemma 2.1. ■

In Part I [2, Theorem 2.5], we showed that the smallest-size commutative ring over which a network is scalar linearly solvable is unique. However, there may exist multiple simple rings of the same size (e.g.  $\text{GF}(p^4)$  and  $M_2(\text{GF}(p))$  are non-isomorphic simple rings of size  $p^4$ ). An interesting open question is whether every network with a scalar linear solution over multiple simple rings of the same size also must have a scalar linear solution over some smaller simple ring. I.e. is the smallest ring  $R$  in Theorem 2.5 unique for a given network?

We demonstrate (in Corollaries 2.14 and 3.8) that for two infinite classes of networks (one of which is a class of multicast networks) studied in this paper, the smallest-size ring over which each network is scalar linearly solvable is unique.

## 2.1 Modules and vector linear codes

The following lemma shows that linear solutions over unfaithful modules admit linear solutions over faithful modules.

**Lemma 2.6.** *Let  $G$  be an  $R$ -module. There exists a ring  $S$  such that  $G$  is a faithful  $S$ -module, and any network that is linearly solvable over  ${}_R G$  is linearly solvable over  ${}_S G$ . If  $R$  is commutative, then there exists a commutative such  $S$ .*

*Proof.* We use ideas from [5, p. 2750] here. Let  $J = \{r \in R : r \cdot g = 0, \forall g \in G\}$ , which is easily verified to be a two-sided ideal of  $R$ . Let  $S = R/J$ . It can also be verified that  $G$  is an  $S$ -module with action  $\odot$  given by  $(r + J) \odot g = r \cdot g$ .

If  $(r + J), (s + J) \in S$  are such that  $(r + J) \odot g = (s + J) \odot g$  for all  $g \in G$ , then  $(r - s) \cdot g = 0$ , which implies  $(r - s) \in J$ . Hence  $(r + J) = (s + J)$ , so the ring  $S$  acts faithfully on  $G$ . If  $R$  is commutative, then the ring  $R/J = S$  is also commutative.

Suppose a network  $\mathcal{N}$  is linearly solvable over  ${}_R G$ . Every edge function in the solution is of the form

$$y' = M_1 \cdot x_1 + \cdots + M_m \cdot x_m \quad (3)$$

where the  $x_i$ 's are the parent node's inputs and the  $M_i$ 's are constants from  $R$ . Form a linear code over  ${}_S G$  replacing each coefficient  $M_i$  in (3) by  $(M_i + J)$ . Let  $y$  be the edge symbol in the code

over  ${}_S G$  corresponding to  $y'$  in the code over  ${}_R G$ . Then

$$\begin{aligned} y &= ((M_1 + J) \odot x_1) \oplus \cdots \oplus ((M_m + J) \odot x_m) \\ &= (M_1 \cdot x_1) \oplus \cdots \oplus (M_m \cdot x_m) = y'. \end{aligned}$$

Thus, whenever an edge function in the solution over  ${}_R G$  outputs the symbol  $y'$ , the corresponding edge function in the code over  ${}_S G$  will output the same symbol  $y'$ . Likewise, whenever  $x$  is an input to an edge function in the solution over  ${}_R G$ , the corresponding input of the corresponding edge function in the code over  ${}_S G$  will be the same symbol  $x$ . The same argument holds for the decoding functions in the code over  ${}_S G$ , so each receiver will correctly obtain its corresponding demands in the code over  ${}_S G$ . Hence, the code over  ${}_S G$  is a linear solution for  $\mathcal{N}$ . ■

In a linear network code over a module  ${}_R G$ , in principle, the ring  $R$  need not be finite (although representing linear code coefficients might be problematic). For example, any Abelian group  $(G, \oplus)$  is a  $\mathbf{Z}$ -module with action given by

$$n \cdot g = \begin{cases} \underbrace{g \oplus \cdots \oplus g}_{n \text{ adds}} & n > 0 \\ (-n) \cdot (-g) & n < 0 \\ 0 & n = 0. \end{cases}$$

However, in a linear network code over a module, the alphabet is finite, so the Abelian group  $G$  must be finite.<sup>3</sup> The following corollary shows that if a network is linearly solvable over a module where the ring is infinite, then it is also linearly solvable over a faithful module where the ring is finite.

**Corollary 2.7.** *Let  $R$  be an infinite ring and let  $G$  be a finite  $R$ -module. Then there exists a finite ring  $S$  such that  $G$  is a faithful  $S$ -module and any network that is linearly solvable over  ${}_R G$  is linearly solvable over  ${}_S G$ . If  $R$  is commutative, then there exists a commutative such  $S$ .*

*Proof.* This follows from Lemma 2.6, and the fact that the ring of a faithful finite module must also be finite. ■

A *submodule* of an  $R$ -module  $G$  is a subgroup  $H$  of  $G$  such that  $H$  is closed when acted on by  $R$ . That is, both  $H$  and  $G$  are  $R$ -modules and  $H \subseteq G$ . Submodules are of particular interest, since by Lemma 1.2, if  $G$  and  $H$  are faithful  $R$ -modules, then the set of networks that are linearly solvable over  ${}_R G$  and the set of networks that are linearly solvable over  ${}_R H$  are equal, yet a linear code over  ${}_R H$  has a smaller alphabet if  $H$  is a proper submodule of  $G$ .

As an example, let  $I$  be a two-sided ideal in the ring  $R$ . Then  $(I, +)$  is a subgroup of  $(R, +)$  that is closed under multiplication in  $R$ , so  ${}_R I$  is a submodule of the  $R$ -module  $R$ . As another example, for each finite field  $\mathbb{F}$  and integer  $k \geq 2$ , the  $M_k(\mathbb{F})$ -module  $\mathbb{F}^k$  is a proper submodule of the  $M_k(\mathbb{F})$ -module  $M_k(\mathbb{F})$ .

Lemmas 2.8 and 2.9 show results related to submodules that will be used to prove Theorem 2.10.

---

<sup>3</sup>We will call a module “finite” if and only if its Abelian group is finite.

**Lemma 2.8.** [12, Theorem 3.3 (2), p. 31] *Let  $\mathbb{F}$  be a finite field and  $k$  a positive integer. Then  $\mathbb{F}^k$  is the only  $M_k(\mathbb{F})$ -module that has no proper submodules.*

By Lemma 1.2, for each ring  $R$ , if a network is linearly solvable over a faithful  $R$ -module, then it is linearly solvable over every  $R$ -module. When a network is solvable over the  $R$ -modules for a particular ring  $R$ , it may be desirable for linear network coding to determine the minimum-size  $R$ -modules. Lemma 2.9 considers this question for rings of matrices over a finite field.

**Lemma 2.9.** *Let  $\mathbb{F}$  be a finite field and  $k$  a positive integer. If  $G$  is a finite non-zero  $M_k(\mathbb{F})$ -module, then  $|\mathbb{F}|^k$  divides  $|G|$ .*

*Proof.* Since  $G$  is finite and non-zero,  $G$  contains a submodule with no proper submodules. By Lemma 2.8,  $\mathbb{F}^k$  is the only  $M_k(\mathbb{F})$ -module with no proper submodules, so  $\mathbb{F}^k$  is a submodule of  $G$ . Hence by Lagrange's theorem of finite groups (e.g. [7, p. 89, Theorem 8]),  $|\mathbb{F}|^k$  divides  $|G|$ . ■

The following theorem is a generalization of Theorem 2.5, where we characterize smallest-size modules over which networks are linearly solvable. Theorem 2.10 demonstrates that if a network is linearly solvable over some module, then there exists a vector linear code over a field that minimizes the alphabet size needed for a linear solution.

**Theorem 2.10.** *Suppose a network  $\mathcal{N}$  is linearly solvable over an  $R$ -module  $G$ . Then the following hold:*

- (a) *There exists a finite field  $\mathbb{F}$  and positive integer  $k$  such that  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$  and  $|\mathbb{F}|^k$  divides  $|G|$ .*
- (b) *If  $R$  is commutative, then there exists a finite field  $\mathbb{F}$  such that  $\mathcal{N}$  has a scalar linear solution over  $\mathbb{F}$  and  $|\mathbb{F}|$  divides  $|G|$ .*

*Proof.* If the ring  $R$  is infinite, then by Corollary 2.7,  $\mathcal{N}$  is linearly solvable over some faithful module with a finite ring. If  $R$  is commutative, then by Corollary 2.7,  $\mathcal{N}$  is linearly solvable over some faithful module with a finite commutative ring. So without loss of generality, assume  $R$  is finite and  $G$  is a faithful  $R$ -module. By Lemmas 2.1 and 2.3 (a), since  $R$  is finite, there exists a field  $\mathbb{F}$ , a positive integer  $k$ , and a surjective homomorphism  $\phi : R \rightarrow M_k(\mathbb{F})$ . By Lemma 1.4 any network that is linearly solvable over the faithful  $R$ -module  $G$  is also linearly solvable over every  $M_k(\mathbb{F})$ -module, so in particular,  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$ . Since  $\phi$  is a homomorphism, any  $R$ -module is also an  $M_k(\mathbb{F})$ -module (see the proof of Lemma 1.4). Thus, both  $G$  and  $\mathbb{F}^k$  are  $M_k(\mathbb{F})$ -modules, so by Lemma 2.9, we have  $|\mathbb{F}|^k$  divides  $|G|$ .

If  $R$  is commutative, then, since  $\phi$  is a surjective homomorphism,  $M_k(\mathbb{F})$  must also be commutative, which implies  $k = 1$ . Hence  $\mathcal{N}$  has a scalar linear solution over  $\mathbb{F}$  and  $|\mathbb{F}|$  divides  $|G|$ . ■

Theorem 2.10 demonstrates that, in some sense, vector linear codes over finite fields are optimal for linear network coding, as they can minimize the alphabet size needed for a linear solution. The following lemmas will be used to show (in Theorem 2.13) that a minimum-size module over which a network is linearly solvable is not necessarily unique. Lemma 2.11 is a result of Sun et. al [16].

**Lemma 2.11.** [16, Proposition 1, p. 4513] *Let  $q$  be a prime power and  $k$  a positive integer. If a network has a scalar linear solution over  $\text{GF}(q^k)$ , then it has a  $k$ -dimensional vector linear solution over  $\text{GF}(q)$ .*

For each integer  $n \geq 3$ , the  $n$ -Choose-Two Network is a multicast network that was described by Rasala Lehman and Lehman [15] and further studied in our Part I (see Figure 1 in [2]).

**Lemma 2.12.** [15, p. 144] *Let  $\mathcal{A}$  be a network alphabet and let integer  $n \geq 3$ .*

- (a) *If the  $n$ -Choose-Two Network has a solution over  $\mathcal{A}$ , then  $|\mathcal{A}| \geq n - 1$ .*
- (b) *Let  $\mathcal{A}$  be a field. The  $n$ -Choose-Two Network is linearly solvable over  $\mathcal{A}$  if and only if  $|\mathcal{A}| \geq n - 1$ .*

**Theorem 2.13.** *For each integer  $k \geq 2$  and prime  $p$ , the  $(p^k + 1)$ -Choose-Two Network is linearly solvable over at least two distinct modules of size  $p^k$  but not over any smaller modules.*

*Proof.* By Lemma 2.12, the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^k)$  and is not solvable over any alphabet whose size is less than  $p^k$ . By Lemma 2.11, any network with a scalar linear solution over  $\text{GF}(p^k)$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . Hence the  $(p^k + 1)$ -Choose-Two Network has a scalar linear solution over  $\text{GF}(p^k)$  and a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ , yet the network has no linear solution over any module whose size is less than  $p^k$ . ■

The following corollary generalizes Theorem 2.11 from Part I, which showed the  $(p^k + 1)$ -Choose-Two Network is not scalar linearly solvable over any commutative ring of size  $p^k$  other than the field  $\text{GF}(p^k)$ . In fact, as a result of Corollary 2.14, the  $(p^k + 1)$ -Choose-Two Network is not scalar linearly solvable over any ring of size  $p^k$  other than the field.

**Corollary 2.14.** *For each integer  $k \geq 2$  and prime  $p$ , the unique smallest-size ring over which the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable is  $\text{GF}(p^k)$ .*

*Proof.* By Lemma 2.12, the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^k)$  and is not solvable over any smaller alphabet.

Suppose the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over a ring  $R$  of size  $p^k$ . By Lemmas 2.1 and 2.3 (a) (b), there exists a field  $\mathbb{F}$ , a positive integer  $n$ , and a surjective homomorphism  $\phi : R \rightarrow M_n(\mathbb{F})$  such that the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over the ring  $M_n(\mathbb{F})$ . Since  $\phi$  is surjective,  $p^k \geq |\mathbb{F}|^{n^2}$ . By Corollary 1.3, the  $(p^k + 1)$ -Choose-Two Network has an  $n$ -dimensional vector linear solution over  $\mathbb{F}$ , so by Lemma 2.12 (a),  $|\mathbb{F}|^n \geq p^k$ .

Hence  $|\mathbb{F}|^n \geq p^k \geq |\mathbb{F}|^{n^2}$ , which implies  $n = 1$  and  $\mathbb{F} = \text{GF}(p^k)$ . Since  $\phi : R \rightarrow \mathbb{F}$  is a surjective homomorphism and  $|\mathbb{F}| = |R|$ , we have  $R \cong \text{GF}(p^k)$ . ■

The following corollaries summarize our results on the linear solvability of networks using scalar and linear vector codes over fields, scalar linear codes over rings, and linear codes over modules. Corollary 2.15 shows an equivalence between vector linear solvability over fields and linear solvability over rings and modules, while Corollary 2.16 shows an equivalence between scalar linear solvability over fields and linear solvability over commutative rings and modules.

**Corollary 2.15.** *For any network  $\mathcal{N}$ , the following three statements are equivalent:*

- (i)  $\mathcal{N}$  is vector linearly solvable over some finite field.

- (ii)  $\mathcal{N}$  is scalar linearly solvable over some ring.
- (iii)  $\mathcal{N}$  is linearly solvable over some module.

*Proof.* If a network has a  $k$ -dimensional vector linear solution over some field  $\mathbb{F}$ , then by Corollary 1.3 it has a scalar linear solution over the ring  $M_k(\mathbb{F})$ , hence (i) implies (ii). A scalar linear code over a ring is a special case of a linear code over a module, so (ii) implies (iii). By Theorem 2.10 (a), (iii) implies (i). ■

**Corollary 2.16.** *For any network  $\mathcal{N}$ , the following three statements are equivalent:*

- (i)  $\mathcal{N}$  is scalar linearly solvable over some finite field.
- (ii)  $\mathcal{N}$  is scalar linearly solvable over some commutative ring.
- (iii)  $\mathcal{N}$  is linearly solvable over some module whose ring is commutative.

*Proof.* A scalar linear code over a finite field is a special case of a scalar linear code over a commutative ring, hence (i) implies (ii). A scalar linear code over a commutative ring is a special case of a linear code over a module where the ring is commutative, so (ii) implies (iii). By Theorem 2.10 (b), (iii) implies (i). ■

We summarize our results on minimizing the alphabet size in linear network coding by:

- If a network is scalar linearly solvable over some commutative ring, then the (unique) smallest such commutative ring is a field [2, Theorem 2.5].
- If a network is scalar linearly solvable over some ring, then a smallest such ring is a matrix ring over field (Theorem 2.5). It is not known whether such a smallest ring is unique.
- If a network is linearly solvable over some module, then a smallest such module yields a vector linear solution over a field (Theorem 2.10). Such a module may not be unique (Theorem 2.13).

### 3 The Dim- $n$ Network

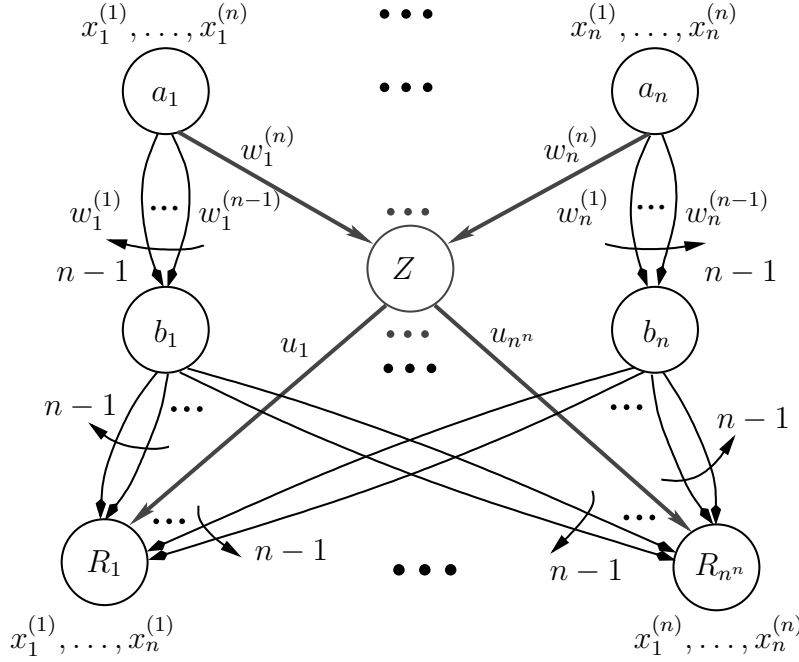


Figure 1: The Dim- $n$  network. For each  $i = 1, \dots, n$ , the node  $a_i$  is a source node that generates messages  $x_i^{(1)}, \dots, x_i^{(n)}$ , and  $a_i$  has  $n - 1$  parallel out-edges to node  $b_i$  and one out-edge to node  $Z$ . For each  $j = 1, \dots, n$ , the receiver  $R_j$  has  $n - 1$  parallel in-edges from each of the nodes  $b_1, \dots, b_n$  and a single in-edge from node  $Z$ . Each receiver demands a single message from each source node and each set of  $n$  messages demanded by each receiver is unique; that is, for any  $i_1, \dots, i_n \in \{1, \dots, n\}$ , there is exactly one receiver which demands  $x_1^{(i_1)}, \dots, x_n^{(i_n)}$ .

For each integer  $n \geq 2$ , the *Dim- $n$  Network* is defined in Figure 1 and is referred to as such because it has vector linear solutions precisely over vector dimensions that are multiples of  $n$ . We prove this fact in Theorem 3.6. This infinite family of networks will be used to demonstrate several theorems related to commutative and non-commutative rings. The special case of  $n = 2$  corresponds to the *M Network* of [14], shown later in Figure 2.

**Remark 3.1.** The Dim- $n$  Network has  $n^n + 2n + 1$  nodes and  $n^n(n^2 - n + 1) + n^2$  edges.

**Lemma 3.2.** For each integer  $n \geq 2$  and alphabet  $\mathcal{A}$ , the Dim- $n$  Network has an  $n$ -dimensional vector routing solution over  $\mathcal{A}$ .

*Proof.* Each message and edge symbol is an element of  $\mathcal{A}^n$ . Let  $[x]_i$  denote the  $i$ th component of  $x \in \mathcal{A}^n$ . Define an  $n$ -dimensional routing code over  $\mathcal{A}$  by

$$\left[ w_i^{(j)} \right]_k = \left[ x_i^{(k)} \right]_j \quad (i, j, k = 1, \dots, n).$$

That is, the  $k$ th component of the  $j$ th out-edge of the  $i$ th source node carries the  $j$ th component of the  $k$ th message originating at the  $i$ th source node.

For each  $i = 1, \dots, n$  and each  $j = 1, \dots, n^n$ , let the set of  $(n-1)$  parallel edges from node  $b_i$  to receiver  $R_j$  carry the symbols  $w_i^{(1)}, \dots, w_i^{(n-1)}$ . Then each receiver gets the first  $(n-1)$  components of every message from the edges originating at  $b_1, \dots, b_n$ , so in particular, each receiver can recover the first  $(n-1)$  components of each of the messages it demands.

Node  $Z$  receives the  $n$ th component of each message, so each of its out-edges can carry any  $n$  of these components. Let  $j \in \{1, \dots, n^n\}$ , suppose  $x_1^{(i_1)}, \dots, x_n^{(i_n)}$  are the messages receiver  $R_j$  demands, and let

$$[u_j]_k = \left[ w_k^{(n)} \right]_{i_k} = \left[ x_k^{(i_k)} \right]_n \quad (k = 1, \dots, n).$$

Then  $R_j$  can recover the  $n$ th component of each of the messages it demands. Since  $j$  was chosen arbitrarily, the code is an  $n$ -dimensional vector routing solution. ■

The following lemmas will be used in later proofs.

**Lemma 3.3.** *Let  $R$  be a finite ring and let  $k_1, \dots, k_n$  be positive integers. If a network has  $k_1, \dots, k_n$ -dimensional vector linear solutions over  $R$ , then the network has a  $(k_1 + \dots + k_n)$ -dimensional vector linear solution over  $R$ .*

*Proof.* Assume a network has a  $k_i$ -dimensional vector linear solution over  $R$  for each  $i = 1, \dots, n$ . In the  $k_i$ -dimensional vector linear solution over  $R$ , every edge function is of the form

$$y^{(i)} = M_1^{(i)} x_1^{(i)} + \dots + M_m^{(i)} x_m^{(i)}$$

where  $x_j^{(i)} \in R^{k_i}$  are the inputs to the node and  $M_j^{(i)}$  are  $k_i \times k_i$  matrices over  $R$ . For any such edge function, define a  $(k_1 + \dots + k_n)$ -dimensional vector linear edge function over  $R$  by letting

$$\begin{bmatrix} y^{(1)} \\ \vdots \\ y^{(n)} \end{bmatrix} = \sum_{j=1}^m \begin{bmatrix} M_j^{(1)} & \mathbf{0} \\ & \ddots \\ \mathbf{0} & & M_j^{(n)} \end{bmatrix} \begin{bmatrix} x_j^{(1)} \\ \vdots \\ x_j^{(n)} \end{bmatrix}.$$

It is straightforward to see this provides a vector linear solution for the network. ■

Let  $X$  and  $Y$  be collections of discrete random variables over alphabet  $\mathcal{A}$ , and let  $p_X$  be the probability mass function of  $X$ . We denote the (base  $|\mathcal{A}|$ ) *entropy* of  $X$  as

$$H(X) = - \sum_u p_X(u) \log_{|\mathcal{A}|} p_X(u)$$

and the *conditional entropy* of  $X$  given  $Y$  as

$$H(X|Y) = H(X, Y) - H(Y).$$

The proof of Theorem 3.6 will make use of Lemmas 3.4 and 3.5 and the following basic information inequalities:

$$H(X|Y) \leq H(X) \quad (4)$$

$$\leq H(X, Y) \quad (5)$$

$$\leq H(X) + H(Y). \quad (6)$$

**Lemma 3.4.** *Let  $X, Y_1, \dots, Y_n$  be collections of discrete random variables. Then*

$$H(X, Y_1) + \dots + H(X, Y_n) \geq (n-1)H(X) + H(X, Y_1, \dots, Y_n).$$

*Proof.*

$$\begin{aligned} \sum_{i=1}^n H(X, Y_i) &= nH(X) + \sum_{i=1}^n H(Y_i|X) \\ &\geq nH(X) + H(Y_1|X) + \sum_{i=2}^n H(Y_i|X, Y_1, \dots, Y_{i-1}) \quad [\text{from (4)}] \\ &= (n-1)H(X) + H(X, Y_1, \dots, Y_n). \end{aligned}$$

■

**Lemma 3.5.** [6, Lemma V.9] *Let  $L : \mathbb{F}^m \rightarrow \mathbb{F}^n$  be a linear map, and let  $x$  be a uniformly distributed random variable on  $\mathbb{F}^m$ . Then  $L(x)$  is uniformly distributed on the range of  $L$ , and the base  $|\mathbb{F}|$  entropy of  $L(x)$  is  $H(L(x)) = \dim(\text{range}(L(x))) \cdot \log |\mathbb{F}|$ .*

**Theorem 3.6.** *For each integer  $n \geq 2$  and each field  $\mathbb{F}$ , the Dim- $n$  Network has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$  if and only if  $n \mid k$ .*

*Proof.* Suppose  $n \mid k$ . Then  $k = nc$  for some integer  $c \geq 1$ . By Lemma 3.2, the Dim- $n$  Network has an  $n$ -dimensional vector linear solution over  $\mathbb{F}$ , so by taking  $k_1 = \dots = k_c = n$  in Lemma 3.3, the Dim- $n$  Network has an  $nc$ -dimensional vector linear solution over  $\mathbb{F}$ .

Conversely, suppose the Dim- $n$  Network has a  $k$ -dimensional vector linear solution over field  $\mathbb{F}$ . Then all messages  $x_i^{(j)}$  and edge symbols  $w_i^{(j)}$  are  $k$ -vectors over  $\mathbb{F}$ . By viewing the message components as independent uniform random variables over  $\mathbb{F}$  and considering the entropy using logarithms base  $|\mathbb{F}|$ , we have

$$H\left(x_1^{(1)}, \dots, x_1^{(n)}, \dots, x_n^{(1)}, \dots, x_n^{(n)}\right) = \sum_{i,j=1}^n H\left(x_i^{(j)}\right). \quad (7)$$

For each  $i = 1, \dots, n$ , the edge symbols  $w_i^{(1)}, \dots, w_i^{(n)}$  are linear functions of  $x_i^{(1)}, \dots, x_i^{(n)}$ , so

$$H\left(w_i^{(1)}, \dots, w_i^{(n)} \mid x_i^{(1)}, \dots, x_i^{(n)}\right) = 0 \quad (i = 1, \dots, n). \quad (8)$$



The receiver  $R_1$  demands the messages  $x_1^{(1)}, \dots, x_n^{(1)}$  and recovers its demands from its in-edges, so

$$H\left(x_1^{(1)}, \dots, x_n^{(1)} \mid w_1^{(1)}, \dots, w_1^{(n-1)}, \dots, w_n^{(1)}, \dots, w_n^{(n-1)}, u_1\right) = 0. \quad (9)$$

For each  $i, j \in \{1, \dots, n\}$ , the edge symbol  $w_i^{(j)}$  is a linear function of only  $x_i^{(1)}, \dots, x_i^{(n)}$ , and the network's messages are jointly independent. Thus,

$$\begin{aligned} & \sum_{i=1}^n H\left(w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(1)}\right) \\ &= H\left(x_1^{(1)}, \dots, x_n^{(1)}, w_1^{(1)}, \dots, w_1^{(n-1)}, \dots, w_n^{(1)}, \dots, w_n^{(n-1)}\right) \quad [\text{from independence}] \\ &\leq H\left(u_1, x_1^{(1)}, \dots, x_n^{(1)}, w_1^{(1)}, \dots, w_1^{(n-1)}, \dots, w_n^{(1)}, \dots, w_n^{(n-1)}\right) \quad [\text{from (5)}] \\ &= H\left(u_1, w_1^{(1)}, \dots, w_1^{(n-1)}, \dots, w_n^{(1)}, \dots, w_n^{(n-1)}\right) \quad [\text{from (9)}] \\ &\leq H(u_1) + \sum_{i=1}^n \sum_{j=1}^{n-1} H\left(w_i^{(j)}\right) \quad [\text{from (6)}] \\ &\leq k(1 + n(n-1)). \end{aligned}$$

By a similar argument, for any  $i_1, \dots, i_n \in \{1, \dots, n\}$ , there exists a receiver which demands the messages  $x_1^{(i_1)}, \dots, x_n^{(i_n)}$ , so

$$\sum_{j=1}^n H\left(w_j^{(1)}, \dots, w_j^{(n-1)}, x_j^{(i_j)}\right) \leq k(n^2 - n + 1). \quad (10)$$

Since  $\bigcup_{j=1}^n \{w_j^{(1)}, \dots, w_j^{(n)}\}$  is a cut-set for each receiver, we have

$$H\left(x_1^{(1)}, \dots, x_1^{(n)}, \dots, x_n^{(1)}, \dots, x_n^{(n)} \mid w_1^{(1)}, \dots, w_1^{(n)}, \dots, w_n^{(1)}, \dots, w_n^{(n)}\right) = 0. \quad (11)$$

Therefore,

$$\begin{aligned}
 kn^2 &= H\left(x_1^{(1)}, \dots, x_1^{(n)}, \dots, x_n^{(1)}, \dots, x_n^{(n)}\right) && \text{[from (7)]} \\
 &\leq H\left(x_1^{(1)}, \dots, x_1^{(n)}, \dots, x_n^{(1)}, \dots, x_n^{(n)}, w_1^{(1)}, \dots, w_1^{(n)}, \dots, w_n^{(1)}, \dots, w_n^{(n)}\right) && \text{[from (5)]} \\
 &= H\left(w_1^{(1)}, \dots, w_1^{(n)}, \dots, w_n^{(1)}, \dots, w_n^{(n)}\right) && \text{[from (11)]} \\
 &\leq \sum_{i=1}^n \sum_{j=1}^n H\left(w_i^{(j)}\right) && \text{[from (6)]} \\
 &\leq kn^2
 \end{aligned}$$

which implies

$$\sum_{i=1}^n \sum_{j=1}^n H\left(w_i^{(j)}\right) = kn^2.$$

But, since  $H\left(w_i^{(j)}\right) \leq k$ , we get

$$H\left(w_i^{(j)}\right) = k \quad (i, j = 1, \dots, n).$$

Also, since  $w_1^{(1)}, \dots, w_1^{(n)}, \dots, w_n^{(1)}, \dots, w_n^{(n)}$  are independent,

$$H\left(w_i^{(1)}, \dots, w_i^{(n-1)}\right) = k(n-1) \quad (i = 1, \dots, n). \quad (12)$$

For each  $i = 1, \dots, n$ , we have

$$\begin{aligned}
 &\sum_{j=1}^n H\left(w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(j)}\right) \\
 &\geq (n-1)H\left(w_i^{(1)}, \dots, w_i^{(n-1)}\right) + H\left(w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(1)}, \dots, x_i^{(n)}\right) && \text{[from Lemma 3.4]} \\
 &= k(n-1)(n-1) + H\left(x_i^{(1)}, \dots, x_i^{(n)}\right) && \text{[from (8), (12)]} \\
 &= k(n^2 - n + 1) && \text{[from (7)]}. \quad (13)
 \end{aligned}$$

By fixing  $i_1 = 1$  and summing over all  $i_2, \dots, i_n$  in (10), we have

$$\begin{aligned}
 & n^{n-1} k (n^2 - n + 1) \\
 & \geq \sum_{i_2, \dots, i_n=1}^n \left( H(w_1^{(1)}, \dots, w_1^{(n-1)}, x_1^{(1)}) + \sum_{j=2}^n H(w_j^{(1)}, \dots, w_j^{(n-1)}, x_j^{(i_j)}) \right) \quad [\text{from (10)}] \\
 & = n^{n-1} H(w_1^{(1)}, \dots, w_1^{(n-1)}, x_1^{(1)}) + n^{n-2} \sum_{j=2}^n \sum_{i=1}^n H(w_j^{(1)}, \dots, w_j^{(n-1)}, x_j^{(i)}) \\
 & \geq n^{n-1} H(w_1^{(1)}, \dots, w_1^{(n-1)}, x_1^{(1)}) + n^{n-2} \sum_{j=2}^n k(n^2 - n + 1) \quad [\text{from (13)}] \\
 & = n^{n-1} H(w_1^{(1)}, \dots, w_1^{(n-1)}, x_1^{(1)}) + n^{n-2} k(n-1)(n^2 - n + 1)
 \end{aligned}$$

and so

$$H(w_1^{(1)}, \dots, w_1^{(n-1)}, x_1^{(1)}) \leq k \left( \frac{n^2 - n + 1}{n} \right).$$

Similarly, for each  $i, j = 1, \dots, n$ , we have

$$H(w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(j)}) \leq k \left( \frac{n^2 - n + 1}{n} \right). \quad (14)$$

However, for each  $i = 1, \dots, n$  we also have

$$\begin{aligned}
 k(n^2 - n + 1) & \leq \sum_{j=1}^n H(w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(j)}) \quad [\text{from (13)}] \\
 & \leq \sum_{j=1}^n k \left( \frac{n^2 - n + 1}{n} \right) \quad [\text{from (14)}] \\
 & = k(n^2 - n + 1)
 \end{aligned}$$

and so for each  $i, j = 1, \dots, n$ ,

$$H(w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(j)}) = k \left( \frac{n^2 - n + 1}{n} \right).$$

The variables  $w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(j)}$  are linear functions of the uniformly distributed messages, so by Lemma 3.5,  $H(w_i^{(1)}, \dots, w_i^{(n-1)}, x_i^{(j)})$  (with logarithms in base  $|\mathbb{F}|$ ) is an integer. However,

$$\gcd(n, n^2 - n + 1) = \gcd(n, (n^2 - n + 1) - n(n - 1)) = \gcd(n, 1) = 1$$

so if  $k \left( \frac{n^2 - n + 1}{n} \right)$  is an integer, then we must have  $n \mid k$ . ■

The following corollary demonstrates it is possible for a network to be scalar linearly solvable over a non-commutative ring but not over any commutative rings, which is, in fact, equivalent to a network being vector linearly solvable over some field but not scalar linearly solvable over any field, by Corollaries 2.15 and 2.16.

**Corollary 3.7.** *For all integers  $n \geq 2$ ,  $k \geq 1$ , and prime  $p$ , the Dim- $n$  Network has a scalar linear solution over a non-commutative ring of size  $p^{kn^2}$  but has no scalar linear solution over any commutative ring.*

*Proof.* If the Dim- $n$  Network were scalar linearly solvable over a commutative ring, then by Corollary 2.16, the Dim- $n$  Network would also be scalar linearly solvable over some finite field. However, by Theorem 3.6, the Dim- $n$  Network is not scalar linearly solvable over any finite field.

By Theorem 3.6, the Dim- $n$  Network has an  $n$ -dimensional vector linear solution over  $\text{GF}(p^k)$ , so by Corollary 1.3 the Dim- $n$  Network has a linear solution over the ring  $M_n(\text{GF}(p^k))$ . ■

**Corollary 3.8.** *For each integer  $n \geq 2$ , the unique smallest-size ring over which the Dim- $n$  Network is scalar linearly solvable is the ring of all  $n \times n$  matrices over  $\text{GF}(2)$ .*

*Proof.* By Theorem 3.6, the Dim- $n$  Network has an  $n$ -dimensional vector linear solution over  $\text{GF}(2)$ , and by Corollary 1.3, the Dim- $n$  Network has a linear solution over the ring  $M_n(\text{GF}(2))$ .

Suppose the Dim- $n$  Network is scalar linearly solvable over a ring  $R$  such that  $|R| \leq 2^{n^2}$ . By Lemmas 2.1 and 2.3 (a) (b) there exists a field  $\mathbb{F}$ , a positive integer  $k$ , and a surjective homomorphism  $\phi : R \rightarrow M_k(\mathbb{F})$  such that the Dim- $n$  Network is scalar linearly solvable over  $M_k(\mathbb{F})$ . By Corollary 1.3, this implies the Dim- $n$  Network has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$ , which by Theorem 3.6, implies  $n$  divides  $k$ . Since  $\phi$  is surjective,  $|M_k(\mathbb{F})| \leq |R|$ . Hence we have

$$2^{n^2} \leq 2^{k^2} \leq |\mathbb{F}|^{k^2} = |M_k(\mathbb{F})| \leq |R| \leq 2^{n^2}.$$

Therefore  $k = n$  and  $\mathbb{F} = \text{GF}(2)$ . Since  $|R| = |M_n(\mathbb{F})|$  and  $\phi$  is a surjective homomorphism, we have  $R \cong M_n(\text{GF}(2))$ . ■

**Example 3.9.** *Setting  $k = 1$  and  $p = n = 2$  in Corollary 3.7 results in the  $M$  Network (see Figure 2) having no scalar linear solution over any commutative ring but having a scalar linear solution over a non-commutative ring of size 16. The non-commutative ring  $M_2(\text{GF}(2))$  consists of all  $2 \times 2$  binary matrices under ordinary matrix addition and multiplication mod 2. Denote the 16 ring elements by:*

$$R_{qrst} = \begin{bmatrix} q & r \\ s & t \end{bmatrix} \quad (q, r, s, t \in \{0, 1\}).$$

*A scalar linear solution for the  $M$  Network over the non-commutative ring  $M_2(\text{GF}(2))$*

(i.e. where  $A, B, C, D, E, F, G, H, W, X, Y, Z \in M_2(\text{GF}(2))$ ) is given by:

$$\begin{array}{ll}
 \text{Edge (1,3)} : A = R_{1000}W + R_{0010}X & \text{Decode at node 6 : } W = R_{1000}A + R_{0010}E + R_{0000}D \\
 \text{Edge (1,4)} : B = R_{0100}W + R_{0001}X & Y = R_{0000}A + R_{0001}E + R_{1000}D \\
 \text{Edge (2,4)} : C = R_{0100}Y + R_{0001}Z & \text{Decode at node 7 : } W = R_{1000}A + R_{0010}F + R_{0000}D \\
 \text{Edge (2,5)} : D = R_{1000}Y + R_{0010}Z & Z = R_{0000}A + R_{0001}F + R_{0100}D \\
 \text{Edge (4,6)} : E = R_{1000}B + R_{0010}C & \text{Decode at node 8 : } X = R_{0100}A + R_{0010}G + R_{0000}D \\
 \text{Edge (4,7)} : F = R_{1000}B + R_{0001}C & Y = R_{0000}A + R_{0001}G + R_{1000}D \\
 \text{Edge (4,8)} : G = R_{0100}B + R_{0010}C & \text{Decode at node 9 : } X = R_{0100}A + R_{0010}H + R_{0000}D \\
 \text{Edge (4,9)} : H = R_{0100}B + R_{0001}C & Z = R_{0000}A + R_{0001}H + R_{0100}D,
 \end{array}$$

where the out-edges of nodes with a single in-edge each carry the symbol on the in-edge, that is, each receiver directly receives the edge symbols  $A$  and  $D$  from the nodes 3 and 5, respectively.

We also note that if the messages and edge symbols of the  $M$  Network are 2-dimensional vectors over  $\text{GF}(2)$ , instead of  $2 \times 2$  binary matrices, then a small modification of the linear code described above provides the 2-dimensional vector linear solution over  $\text{GF}(2)$  given in [14]. This agrees with Corollary 1.3.

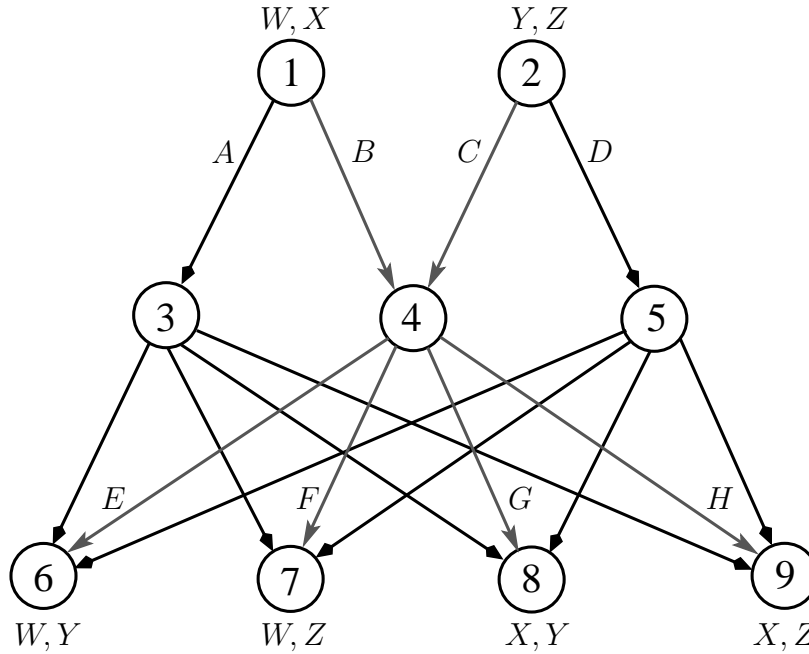


Figure 2: The  $M$  network has a non-commutative scalar linear solution. The messages  $W, X, Y, Z$  take values in  $M_2(\text{GF}(2))$ . The variables  $A, B, C, D, E, F, G, H$  also take values in  $M_2(\text{GF}(2))$  and represent the symbols carried on the 8 indicated edges.

The bound in the following theorem is tight via Example 3.9.

**Theorem 3.10.** *If a network is scalar linearly solvable over some non-commutative ring  $R$ , but not over any commutative rings, then  $|R| \geq 16$ .*

*Proof.* Suppose network  $\mathcal{N}$  is scalar linearly solvable over some non-commutative ring  $R$  and is not linearly solvable over any commutative ring. By Theorem 2.5, there exists a positive integer  $k$  and a field  $\mathbb{F}$  such that  $\mathcal{N}$  has a linear solution over  $M_k(\mathbb{F})$  and  $|R| \geq |M_k(\mathbb{F})|$ . If  $k = 1$ , then  $\mathcal{N}$  is linearly solvable over a field, which contradicts the assumption that  $\mathcal{N}$  is not linearly solvable over any commutative ring. So  $k \geq 2$ , which implies  $|R| \geq |M_k(\mathbb{F})| = |\mathbb{F}|^{k^2} \geq 2^4 = 16$ . ■

## 4 Modules with the same alphabet size

The following theorem demonstrates that there exists a network that is linearly solvable over a module of size  $p^k$  but not over any ring of size  $p^k$ .

**Theorem 4.1.** *For each integer  $k \geq 2$  and prime  $p$ , the Dim- $k$  Network has a  $k$ -dimensional vector linear solution over the field  $\text{GF}(p)$  but is not scalar linearly solvable over any ring of size  $p^k$ .*

*Proof.* By Theorem 3.6, the Dim- $k$  Network has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . Let  $R$  be a ring of size  $p^k$  and suppose the Dim- $k$  Network has a scalar linear solution over  $R$ . By Lemmas 2.1 and 2.3 (b) (c), there exists a field  $\mathbb{F}$  and a positive integer  $n$  such that any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $M_n(\mathbb{F})$  and  $|\mathbb{F}|^{n^2}$  divides  $p^k$ . Hence  $\mathbb{F}$  is a field of characteristic  $p$  and  $n^2 \leq k$ .

Since the Dim- $k$  Network is scalar linearly solvable over  $R$ , the Dim- $k$  Network is scalar linearly solvable over the ring  $M_n(\mathbb{F})$ . By Corollary 1.3, this implies the Dim- $k$  Network has an  $n$ -dimensional vector linear solution over  $\mathbb{F}$ , which by Theorem 3.6 implies  $k \mid n$ . However, this contradicts the fact that  $n^2 \leq k$ . Thus, no such ring  $R$  exists. ■

### 4.1 Commutative rings

Both a scalar linear code over a ring of size  $p^k$  and a  $k$ -dimensional vector linear code are linear codes over a module of size  $p^k$ . We have already seen (in Theorem 4.1) that there exists a network with a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$  yet with no scalar linear solutions over any ring of size  $p^k$ . The main result of this section (Theorem 4.4) will show that any network that is scalar linearly solvable over a commutative ring of size  $p^k$  must also have a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ .

The following lemma was proved in Part I (in [2, Lemmas 2.6 and 5.4]) and will be used in what follows.

**Lemma 4.2.** *For each prime  $p$  and positive integer  $k$ , if a network  $\mathcal{N}$  has a scalar linear solution over some commutative ring of size  $p^k$ , then there exists an integer partition  $(n_1, \dots, n_r)$  of  $k$  such that  $\mathcal{N}$  is scalar linearly solvable over each of the fields  $\text{GF}(p^{n_1}), \dots, \text{GF}(p^{n_r})$ .*

The following standard result on rings will be used in later proofs.

**Lemma 4.3.** [13, Theorem I.1] *Every finite ring is isomorphic to a direct product of rings of prime power sizes.*

**Theorem 4.4.** *Let  $m$  be a positive integer with prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ . If a network  $\mathcal{N}$  has a scalar linear solution over some commutative ring of size  $m$ , then the following hold:*

- (a) *For each  $i = 1, \dots, t$ , network  $\mathcal{N}$  has a  $k_i$ -dimensional vector linear solution over  $\text{GF}(p_i)$ .*
- (b) *Network  $\mathcal{N}$  has a linear solution over the*

$$M_{k_1}(\text{GF}(p_1)) \times \cdots \times M_{k_t}(\text{GF}(p_t))\text{-module } \text{GF}(p_1)^{k_1} \times \cdots \times \text{GF}(p_t)^{k_t}.$$

*Proof.* Suppose  $\mathcal{N}$  is scalar linearly solvable over a commutative ring  $R$  of size  $m$ . By Lemma 4.3, there exist rings  $R_1, \dots, R_t$  such that  $R \cong R_1 \times \dots \times R_t$  and  $|R_i| = p_i^{k_i}$  for all  $i$ .

Let  $i \in \{1, \dots, t\}$ . Since the projection mapping from  $R$  to  $R_i$  is a surjective homomorphism, by Corollary 1.5, network  $\mathcal{N}$  is scalar linearly solvable over  $R_i$ . Then by Lemma 4.2, there exists an integer partition  $(n_1, \dots, n_r)$  of  $k_i$  such that  $\mathcal{N}$  is scalar linearly solvable over each of the fields  $\text{GF}(p_i^{n_1}), \dots, \text{GF}(p_i^{n_r})$ . By Lemma 2.11, this implies that  $\mathcal{N}$  has an  $n_j$ -dimensional vector linear solution over  $\text{GF}(p_i)$  for each  $j = 1, \dots, r$ . However, by Lemma 3.3, this then implies that  $\mathcal{N}$  has a  $k_i = (n_1 + \dots + n_r)$ -dimensional vector linear solution over  $\text{GF}(p_i)$ .

Hence, for all  $i \in \{1, \dots, t\}$ , a Cartesian product code formed from the  $k_i$ -dimensional vector linear solutions over  $\text{GF}(p_i)$  gives a linear solution to  $\mathcal{N}$  over the described module. ■

In Part I, we showed (in [2, Theorems 5.8 and 5.9]) that with respect to ring domination for scalar linear coding, some ring sizes give rise to multiple maximal commutative rings whereas other ring sizes yield only a single unique maximal commutative ring. If there is just one maximal commutative ring of size  $m$ , then every network that is linearly solvable over some commutative ring of size  $m$  is also linearly solvable over the maximal ring. In contrast, if there are multiple maximal commutative rings of size  $m$ , then for any commutative ring  $R$  of size  $m$ , there is always a different commutative ring  $S$  also of size  $m$ , such that some network is scalar linearly solvable over  $S$  but not over  $R$ . Thus, in this sense, there is no “best” commutative ring of a given size.

However, by Theorem 4.4 (b), if a network has a linear solution over some commutative ring of size  $m = p_1^{k_1} \dots p_t^{k_t}$ , then it has a linear solution over the  $M_{k_1}(\text{GF}(p_1)) \times \dots \times M_{k_t}(\text{GF}(p_t))$ -module  $\text{GF}(p_1)^{k_1} \times \dots \times \text{GF}(p_t)^{k_t}$ , which also has size  $m$ . In fact, we showed (in Theorem 4.1) that when  $m = p^k$ , the converse is not true. So in this sense,  $k$ -dimensional vector linear codes over  $\text{GF}(p)$  are strictly “better” than scalar linear codes over commutative rings of size  $p^k$ .

## 4.2 Non-commutative rings

This section generalizes the results of Theorem 4.4 to (not necessarily commutative) rings of size  $m$  with prime factor multiplicity less than or equal to 6. In order to do so, we first will prove some intermediate results and consider special cases.

The following lemma was proved in Part I (in [2, Theorem 5.9]) and will be used in what follows.

**Lemma 4.5.** *For each  $k \in \{1, 2, 3, 4, 6\}$  and prime  $p$ , if a network is scalar linearly solvable over some commutative ring of size  $p^k$ , then it is scalar linearly solvable over  $\text{GF}(p^k)$ .*

Lemma 4.6 characterizes the non-commutative rings of prime-power size whose multiplicity is at most three.

**Lemma 4.6.** [9, pp. 512–513] *For each prime  $p$ , all rings of size  $p$  and of size  $p^2$  are commutative, and the ring of all upper-triangular  $2 \times 2$  matrices over  $\text{GF}(p)$  is the only non-commutative ring of size  $p^3$ .*

We remark that there exist rings of size  $p$  and  $p^2$  without identity. For example, the set  $\{0, 2, 4, 6\}$  with mod 8 addition and multiplication satisfies all of the properties of a ring except



there is no multiplicative identity. However, such rings (sometimes called “rngs”) do not appear to be practical for linear network coding, as receivers must recover their demands from linear combinations of their inputs.

For example, consider the trivial network shown in Figure 3 consisting of a single message  $x$  emitted by a source directly connected by a single edge to a receiver demanding message  $x$ . The only possible linear functions that can be carried on the edge are of the form  $cx$  for some fixed  $c \in \{0, 2, 4, 6\}$ . However, no matter what the choice of  $c$  is, the messages 0 and 4 always get received as 0 mod 8, so the receiver cannot uniquely determine  $x$  in general. Thus, there is no linear solution for the network over this ring (with no multiplicative identity). A similar issue arises for the set  $\{0, 2\}$  with mod 4 addition and multiplication, which also satisfies all of the properties of a ring except there is no multiplicative identity.

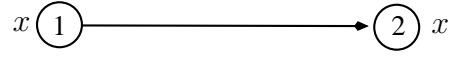


Figure 3: A trivial network with one message  $x$  that is demanded by the receiver.

**Lemma 4.7.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^2$ , then it is a scalar linearly solvable over  $\text{GF}(p^2)$ .*

*Proof.* By Lemma 4.6, every ring of size  $p^2$  is commutative, and by Lemma 4.5, every network that is scalar linearly solvable over some commutative ring of size  $p^2$  has a scalar linear solution over  $\text{GF}(p^2)$ . ■

By Lemma 4.6, the smallest non-commutative ring is the ring of the 8 binary upper-triangular  $2 \times 2$  matrices. As a special case of the following lemma, any network that is scalar linearly solvable over this ring must also have a scalar linear solution over  $\text{GF}(2)$ .

**Lemma 4.8.** *For each finite field  $\mathbb{F}$  and integer  $k \geq 2$ , any network that is scalar linearly solvable over the ring of upper-triangular  $k \times k$  matrices over  $\mathbb{F}$  is also scalar linearly solvable over  $\mathbb{F}$ .*

*Proof.* Let  $R$  be the ring of upper-triangular  $k \times k$  matrices with entries in  $\mathbb{F}$  and let  $\phi : R \rightarrow \mathbb{F}$  be given by

$$\phi \left( \begin{bmatrix} a_{1,1} & \cdots & a_{1,k} \\ & \ddots & \vdots \\ \mathbf{0} & & a_{k,k} \end{bmatrix} \right) = a_{1,1}.$$

Then  $\phi$  is clearly surjective and preserves identities, and for any  $A, B \in R$ ,

$$\begin{aligned} \phi(A + B) &= a_{1,1} + b_{1,1} = \phi(A) + \phi(B) \\ \phi(AB) &= a_{1,1} b_{1,1} = \phi(A)\phi(B). \end{aligned}$$

Thus  $\phi$  is a surjective homomorphism, so by Corollary 1.5, any network that is scalar linearly solvable over  $R$  is scalar linearly solvable over  $\mathbb{F}$ . ■

**Lemma 4.9.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^3$ , then it is scalar linearly solvable over  $\text{GF}(p^3)$ .*

*Proof.* By Lemma 4.6, the only non-commutative ring of size  $p^3$  is the ring of upper triangular matrices with entries in  $\text{GF}(p)$ , and by Lemma 4.8, any network that is scalar linearly solvable over this ring is also scalar linearly solvable over  $\text{GF}(p)$ . Since  $\text{GF}(p)$  is a subring of  $\text{GF}(p^3)$ , any network that is scalar linearly solvable over  $\text{GF}(p)$  is scalar linearly solvable over  $\text{GF}(p^3)$ .

By Lemma 4.5, every network that is scalar linearly solvable over some commutative ring of size  $p^3$  has a scalar linear solution over  $\text{GF}(p^3)$ . ■

The following three lemmas are proved in the Appendix.

**Lemma 4.10.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^4$ , then it is scalar linearly solvable over at least one of the rings  $\text{GF}(p^4)$  or  $M_2(\text{GF}(p))$ .*

**Lemma 4.11.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^5$ , then it is scalar linearly solvable over at least one of the rings  $\text{GF}(p^5)$  or  $\text{GF}(p^3) \times \text{GF}(p^2)$ .*

**Lemma 4.12.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^6$ , then it is scalar linearly solvable over  $\text{GF}(p^6)$ .*

Theorem 4.13 is a generalization of Lemma 4.5 to scalar linear codes over non-commutative rings. Extending Theorem 4.13 to  $|R| = p^k$  for  $k \geq 7$  is left as an open problem.

**Theorem 4.13.** *Let  $p$  be a prime, and suppose  $\mathcal{N}$  is scalar linearly solvable over a ring  $R$ .*

- (a) *If  $|R| = p^2$ , then  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^2)$ .*
- (b) *If  $|R| = p^3$ , then  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^3)$ .*
- (c) *If  $|R| = p^4$ , then  $\mathcal{N}$  is scalar linearly solvable over at least one of  $\text{GF}(p^4)$  or  $M_2(\text{GF}(p))$ .*
- (d) *If  $|R| = p^5$ , then  $\mathcal{N}$  is scalar linearly solvable over at least one of  $\text{GF}(p^5)$  or  $\text{GF}(p^3) \times \text{GF}(p^2)$ .*
- (e) *If  $|R| = p^6$ , then  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^6)$ .*

*Proof.* This follows immediately from Lemmas 4.7, 4.9, 4.10, 4.11, and 4.12. ■

We also note that by Corollary 2.14, the  $(p^4 + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^4)$  but not over  $M_2(\text{GF}(p))$  and the  $(p^5 + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^5)$  but not over  $\text{GF}(p^3) \times \text{GF}(p^2)$ . By Corollary 3.7, the Dim-2 Network is scalar linearly solvable over  $M_2(\text{GF}(p))$  but not over  $\text{GF}(p^4)$ . We showed in Part I [2, Theorem 3.10] that there exists a network that is scalar linearly solvable over  $\text{GF}(p^3) \times \text{GF}(p^2)$  but not over  $\text{GF}(p^5)$ . Hence it is necessary to include both rings in (c) and (d) in Theorem 4.13.

**Corollary 4.14.** *Let  $p$  be a prime and  $k \in \{2, 3, 4, 5, 6\}$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over a ring of size  $p^k$ . Then  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ .*

*Proof.* If  $k \in \{2, 3, 5, 6\}$ , then by Theorem 4.13,  $\mathcal{N}$  has a scalar linear solution over a commutative ring of size  $p^k$ , so by Theorem 4.4,  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ .

Now suppose  $k = 4$ . If  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^4)$ , then by Lemma 2.11,  $\mathcal{N}$  has a 4-dimensional vector linear solution over  $\text{GF}(p)$ . If  $\mathcal{N}$  is not scalar linearly solvable over  $\text{GF}(p^4)$ , then by Theorem 4.13 (c),  $\mathcal{N}$  must be scalar linearly solvable over  $M_2(\text{GF}(p))$ , so by Corollary 1.3,  $\mathcal{N}$  has a 2-dimensional vector linear solution over  $\text{GF}(p)$ , in which case  $\mathcal{N}$  also has a 4-dimensional vector linear solution over  $\text{GF}(p)$  by Lemma 3.3. ■

Theorem 4.15 generalizes the results of Theorem 4.4 to rings of size  $m$  with prime factor multiplicity less than or equal to 6.

**Theorem 4.15.** *Let  $m$  be a positive integer with prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ . If a network  $\mathcal{N}$  has a scalar linear solution over a ring of size  $m$ , then, for each  $i = 1, \dots, t$  such that  $k_i \leq 6$ , network  $\mathcal{N}$  has a  $k_i$ -dimensional vector linear solution over  $\text{GF}(p_i)$ .*

*Proof.* Suppose  $\mathcal{N}$  is scalar linearly solvable over a ring  $R$  of size  $m$ . By Lemma 4.3, there exists rings  $R_1, \dots, R_t$  such that  $R \cong R_1 \times \cdots \times R_t$  and  $|R_i| = p_i^{k_i}$  for all  $i$ .

Now, let  $i \in \{1, \dots, t\}$  and suppose  $k_i \leq 6$ . The projection mapping from  $R$  to  $R_i$  is a surjective homomorphism, so by Corollary 1.5, network  $\mathcal{N}$  is scalar linearly solvable over  $R_i$ . Since  $\mathcal{N}$  is scalar linearly solvable over a ring of size  $p_i^{k_i}$  where  $k_i \leq 6$ , by Corollary 4.14,  $\mathcal{N}$  has a  $k_i$ -dimensional vector linear solution over  $\text{GF}(p_i)$ . ■

We leave as an open question whether the restriction that  $k_i \leq 6$  can be removed from the statement of Theorem 4.15. If this generalization is false, then for what primes  $p$  and positive integers  $k$  is it the case that there exists a network with a scalar linear solution over a ring of size  $p^k$  but with no  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ ? If such a ring and such a network do exist, the ring must be non-commutative and  $k \geq 7$ . More generally, does there exist a network with a linear solution over some alphabet of size  $p^k$  but with no  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ ?

## 5 Concluding Remarks

For each positive integer  $k$  and prime  $p$ , we have shown the set

$$\{\mathcal{N} : \mathcal{N} \text{ has a scalar linear solution over some commutative ring of size } p^k\}$$

is properly contained in

$$\{\mathcal{N} : \mathcal{N} \text{ has a } k\text{-dimensional vector linear solution over } \text{GF}(p)\}.$$

So in this sense,  $k$ -dimensional vector linear codes over  $\text{GF}(p)$  may be advantageous compared to scalar linear codes over commutative rings of the same size  $p^k$ . In addition, there are more  $k$ -dimensional linear functions over  $\text{GF}(p)$  than there over a commutative ring of size  $p^k$ . Vector linear codes over fields are also optimal in the sense that they minimize the alphabet size needed for a linear solution over a particular network. On the other hand, the complexity of implementing vector linear codes is generally higher than for scalar linear codes over commutative rings of the same size.

## Appendix

The main purpose of this Appendix is to prove Lemmas 4.10, 4.11, and 4.12, which are used in the proof of Theorem 4.13. It is an open question whether Theorem 4.15 can be extended to all finite rings. The techniques presented in this section may additionally be useful for examining such questions.

Recall that a finite ring is simple if it has no proper two-sided ideals. The *radical* of a ring  $R$  is the intersection of all its maximal left ideals. The radical of a ring is a two-sided ideal. A finite ring  $R$  with radical  $J$  is said to be:

- *local*<sup>4</sup> if  $R/J$  is a field.
- *semi-local* if  $R/J$  is simple, or equivalently  $R$  is isomorphic to a matrix over a local ring (e.g. [13, p. 162]).
- *semi-simple* if  $R$  is isomorphic to a direct product of simple rings (matrix rings over fields) or equivalently,  $J = \{0\}$  (e.g. [13, pp. 75, 128]).

The following lemma is a result on local rings that will be used in later proofs.

**Lemma A.1.** *Let  $p$  be a prime,  $k$  a positive integer, and  $R$  a semi-local ring of size  $p^k$ . Then there exists a unique local ring  $S$  and positive integers  $r, s, t$  such that the following hold:*

- (a) [13, Theorem VIII.26]  $R \cong M_r(S)$
- (b) [1, Theorem 6.1.2]  $|S| = p^s$
- (c) [1, Theorem 6.1.2]  $\text{GF}(p^t) \cong S/J$ , where  $J$  is the radical of  $S$  and  $t \mid s$ .

As an example, let  $p$  be a prime and let  $r, s$  be positive integers. Then  $M_r(\mathbb{Z}_{p^s})$  is a semi-local ring, since  $\mathbb{Z}_{p^s}$  is a local ring. We also remark that in Lemma A.1, if  $R$  is itself local, then  $S \cong R$ .

The following lemmas are results on semi-simple rings and the radicals of rings.

**Lemma A.2.** [13, Proposition IV.6, Theorem VIII.4] *Let  $R$  be a finite ring with radical  $J$ . Then there exist fields  $\mathbb{F}_1, \dots, \mathbb{F}_s$  and positive integers  $r_1, \dots, r_s$  such that*

$$R/J \cong M_{r_1}(\mathbb{F}_1) \times \dots \times M_{r_s}(\mathbb{F}_s).$$

**Lemma A.3.** *Let  $R$  be a finite ring with radical  $J$ , and suppose*

$$R/J \cong M_{r_1}(\mathbb{F}_1) \times \dots \times M_{r_s}(\mathbb{F}_s)$$

*for some fields  $\mathbb{F}_1, \dots, \mathbb{F}_s$  and positive integers  $r_1, \dots, r_s$ . If a network is scalar linearly solvable over  $R$ , then it is also scalar linearly solvable over each of the rings  $M_{r_1}(\mathbb{F}_1), \dots, M_{r_s}(\mathbb{F}_s)$ .*

---

<sup>4</sup>If  $R$  is a local commutative ring, then  $R$  has a single maximal ideal, which corresponds to our definition of a commutative local ring in Part I.

*Proof.* By Lemma 2.2, there exists a surjective homomorphism  $\phi : R \rightarrow R/J$ . Let  $i \in \{1, \dots, s\}$ . Then the projection mapping  $\psi_i : R/J \rightarrow M_{r_i}(\mathbb{F}_i)$  is a surjective homomorphism. Hence the composition of mappings  $\psi_i \circ \phi : R \rightarrow M_{r_i}(\mathbb{F}_i)$  is a surjective homomorphism. Thus by Corollary 1.5, any network with a scalar linear solution over  $R$  has a scalar linear solution over the ring  $M_{r_i}(\mathbb{F}_i)$ . ■

The following is an enumeration of semi-simple rings that we will reference in upcoming proofs. For each prime  $p$ , it can be verified that the rings given in (15)–(47) are all of the semi-simple rings of sizes  $p, p^2, p^3, p^4, p^5$ , or  $p^6$  (up to isomorphism).

$$\text{Size } p : \text{GF}(p) \tag{15}$$

$$\text{Size } p^2 : \text{GF}(p^2) \tag{16}$$

$$\text{GF}(p) \times \text{GF}(p) \tag{17}$$

$$\text{Size } p^3 : \text{GF}(p^3) \tag{18}$$

$$\text{GF}(p^2) \times \text{GF}(p) \tag{19}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{20}$$

$$\text{Size } p^4 : M_2(\text{GF}(p)) \tag{21}$$

$$\text{GF}(p^4) \tag{22}$$

$$\text{GF}(p^3) \times \text{GF}(p) \tag{23}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \tag{24}$$

$$\text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \tag{25}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{26}$$

$$\text{Size } p^5 : \text{GF}(p^5) \tag{27}$$

$$M_2(\text{GF}(p)) \times \text{GF}(p) \tag{28}$$

$$\text{GF}(p^4) \times \text{GF}(p) \tag{29}$$

$$\text{GF}(p^3) \times \text{GF}(p^2) \tag{30}$$

$$\text{GF}(p^3) \times \text{GF}(p) \times \text{GF}(p) \tag{31}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \times \text{GF}(p) \tag{32}$$

$$\text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{33}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{34}$$

$$\text{Size } p^6 : \text{GF}(p^6) \tag{35}$$

$$\text{GF}(p^5) \times \text{GF}(p) \tag{36}$$

$$M_2(\text{GF}(p)) \times \text{GF}(p^2) \tag{37}$$

$$\text{GF}(p^4) \times \text{GF}(p^2) \tag{38}$$

$$M_2(\text{GF}(p)) \times \text{GF}(p) \times \text{GF}(p) \tag{39}$$

$$\text{GF}(p^4) \times \text{GF}(p) \times \text{GF}(p) \tag{40}$$

$$\text{GF}(p^3) \times \text{GF}(p^3) \tag{41}$$

$$\text{GF}(p^3) \times \text{GF}(p^2) \times \text{GF}(p) \tag{42}$$

$$\text{GF}(p^3) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{43}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \times \text{GF}(p^2) \tag{44}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \tag{45}$$

$$\text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{46}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{47}$$

We now prove Lemmas 4.10, 4.11, and 4.12.

*Proof of Lemma 4.10.* Let  $R$  be a ring of size  $p^4$  with radical  $J$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over  $R$ . Then  $|R/J| \in \{p, p^2, p^3, p^4\}$ , so by Lemma A.2,  $R/J$  is isomorphic to one of the rings in (15)–(26).

If  $R/J$  is isomorphic to any of these rings except those in (18) and (21), then by Lemma A.3,  $\mathcal{N}$  is also scalar linearly solvable over at least one of  $\text{GF}(p)$ ,  $\text{GF}(p^2)$ , or  $\text{GF}(p^4)$ . Since  $\text{GF}(p)$  and  $\text{GF}(p^2)$  are both subrings of  $\text{GF}(p^4)$ , in these cases,  $\mathcal{N}$  is also scalar linearly solvable over  $\text{GF}(p^4)$ .

If  $R/J$  is isomorphic to the ring in (21), then by Lemma A.3,  $\mathcal{N}$  is also scalar linearly solvable over  $M_2(\text{GF}(p))$ . It follows from Lemma A.1 that  $R/J$  is not isomorphic to the ring in (18). ■

*Proof of Lemma 4.11.* Let  $R$  be a ring of size  $p^5$  with radical  $J$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over  $R$ . Then  $|R/J| \in \{p, p^2, p^3, p^4, p^5\}$ , so by Lemma A.2,  $R/J$  must be isomorphic to one of the rings in (15)–(34).

If  $R/J$  is isomorphic to one of the rings in (21)–(26) (i.e.  $|R/J| = p^4$ ), then  $|J| = p$ . Since  $(J, +)$  is an  $R$ -module and  $\mathcal{N}$  has a linear solution over the faithful module  ${}_R R$ , by Lemma 1.2,  $\mathcal{N}$  has a linear solution over  ${}_R J$ . By Theorem 2.10, this implies  $\mathcal{N}$  has a scalar linear solution over  $\text{GF}(p)$ . Since  $\text{GF}(p)$  is a subring of  $\text{GF}(p^5)$ , in these cases,  $\mathcal{N}$  also has a scalar linear solution over  $\text{GF}(p^5)$ .

It follows from Lemma A.1 that  $R/J$  is not isomorphic to either of the rings in (16) or (18). If  $R/J$  is isomorphic to the ring in (30), then by Lemma A.3,  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^3) \times \text{GF}(p^2)$ .

If  $R/J$  is isomorphic to any of the remaining cases, then by Lemma A.3, network  $\mathcal{N}$  is scalar linearly solvable over either  $\text{GF}(p)$  or  $\text{GF}(p^5)$ . Since  $\text{GF}(p)$  is a subring of  $\text{GF}(p^5)$ , in these cases,  $\mathcal{N}$  also has a scalar linear solution over  $\text{GF}(p^5)$ . ■

*Proof of Lemma 4.12.* Let  $R$  be a ring of size  $p^6$  with radical  $J$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over  $R$ . Then  $|R/J| \in \{p, p^2, p^3, p^4, p^5, p^6\}$ , so by Lemma A.2,  $R/J$  must be isomorphic to one of the rings in (15)–(47). It follows from Lemma A.1 that  $R/J$  is not isomorphic to any of the rings in (21), (22), or (27).

If  $R/J$  is isomorphic to any of the remaining cases, then it follows from Lemma A.3 that  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^n)$  for some  $n \in \{1, 2, 3, 6\}$ . Since  $n \mid 6$ ,  $\text{GF}(p^n)$  is a subring of  $\text{GF}(p^6)$ , which implies  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^6)$ . ■



## References

- [1] G. Bini and F. Flamini, *Finite commutative rings and their applications*, Kluwer Academic Publishers, 2002.
- [2] J. Connelly and K. Zeger, “Linear network coding over rings, Part I: Scalar codes and commutative alphabets,” submitted to *IEEE Transactions on Information Theory*, Available on-line at: <http://arxiv.org/abs/1608.01738>.
- [3] B. Corbas and G. D. Williams, “Rings of order  $p^5$  part I. Nonlocal rings,” *Journal of Algebra*, vol. 231, no. 2, pp. 677–690, 2000.
- [4] B. Corbas and G. D. Williams, “Rings of order  $p^5$  part II. Local rings,” *Journal of Algebra*, vol. 231, no. 2, pp. 691–704, 2000.
- [5] R. Dougherty, C. Freiling, and K. Zeger, “Insufficiency of linear coding in network information flow,” *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2745–2759, August 2005.
- [6] R. Dougherty, C. Freiling, and K. Zeger, “Networks, matroids, and non-Shannon information inequalities,” *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949–1969, June 2007.
- [7] D. Dummit and R. Foote, *Abstract Algebra*, Third Edition, Hoboken, NJ, John Wiley and Sons Inc., 2004.
- [8] J.B. Ebrahimi and C. Fragouli, “Algebraic algorithms for vector network coding,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996–1007, February 2011.
- [9] K.E. Eldridge, “Orders for finite noncommutative rings with unity,” *The American Mathematical Monthly*, vol. 75, no. 5, pp. 512–514, May 1968.
- [10] B. Fine, “Classification of Finite Rings of Order  $p^2$ ,” *Mathematics Magazine*, vol. 66, no. 4, pp. 248–252, October 1993.
- [11] J. Gathen and J. Gerhard, *Modern Computer Algebra*, Third Edition, Cambridge University Press, 2003.
- [12] T.Y. Lam, *A First Course in Noncommutative Rings*, Second Edition, Springer Verlag New York Inc., 2001.
- [13] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., 1974.
- [14] M. Médard, M. Effros, T. Ho, and D. Karger, “On coding for non-multicast networks,” *Conference on Communication Control and Computing*, Monticello, IL, October 2003.
- [15] A. Rasala Lehman and E. Lehman, “Complexity classification of network information flow problems,” *ACM-SIAM Symposium on Discrete algorithms*, 2004.

- [16] Q. Sun, X. Yangy, K. Long, X. Yin, and Z. Li, “On vector linear solvability of multicast networks,” *IEEE International Conference on in Communications (ICC)*, pp.4511–4517, 8-12 June 2015.